REMARKS

The Office Action dated December 2, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 6 and 31 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter is added. The amendments presented above do not require any additional search or consideration. As such, Applicants submit claims 1-3, 5-8, 12, 26, 28, 29, 31-33, 35 and 37-57 for consideration in view of the following.

As a preliminary matter, Applicants appreciatively acknowledge the Examiner's participation in the examiner interview held on March 16, 2009. During the interview, Applicants and the Examiner discussed distinctions between claimed invention and Pirttimaa. While an agreement was not reached as to the distinctions discussed, Applicants are, nevertheless, appreciative of the Examiners willingness and availability to address the issues raised in the prosecution of this application.

The Office Action objected to the specification as failing to provide antecedent basis for the "computer-readable medium" recited in claim 40-41. Applicants respectfully traverse this objection on the grounds that the specification provides sufficient support for a "computer-readable medium," as recited in claims 40-41.

MPEP 608.01(o) states that "[t]he meaning of every term used in any of the claims should be apparent from the descriptive portion of the specification with clear disclosure

as to its import; and in mechanical cases, it should be identified in the descriptive portion of the specification by reference to the drawing, designating the part or parts therein to which the term applies." However, while the MPEP requires that the terms used in a claim be supported by the specification, the MPEP does not require that each term be recited verbatim. Rather, as stated in MPEP 608.01(o), the MPEP only requires that the specification provide "clear support" for the terms used in a claim.

In compliance with MPEP 608.01(o), the specification of the pending application provides clear support for a computer-readable medium, as recited in claims 40-41. For example, paragraph 21 of the specification discloses a communication system that includes a radio access network and a core network, which are each known to include several devices, such as servers, base station controllers, and mobile device, that store or embody computer programs in memory. Additionally, paragraph 23 discloses a serving general packet radio service support node entity, and paragraph 25 discloses a home subscriber server that are each known to store computer programs. Further, paragraph 30 discloses a user equipment establishing security associations, which are widely known to execute software instructions stored in memory. Indeed, the lengthy specification contains significant information regarding devices that operate by executing software programs that are stored in the devices. A person of ordinary skill in the art would understand these devices as including computer readable media.

Application No.: 10/615,419

Accordingly, the specification provides clear support a "computer-readable medium," as recited in claims 40-41. Consequently, Applicants respectfully request that this rejection be withdrawn.

Claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Publication No. 2003/0154400 ("Pirttimaa"). Applicants respectfully assert that claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 are not anticipated by Pirttimaa under 35 U.S.C. § 102(e).

Claim 1, upon which claims 2-3, 58, 12, 28, and 33 depend, is directed to a method that includes forwarding a prefix value to a node in a packet switched environment to create a security association with the node based on the prefix value. The prefix value may refer to a portion of a first internet protocol address, where the security association is valid for a plurality of different internet protocol addresses. Additionally, each of the plurality of internet protocol addresses comprises the portion of the first internet protocol address to which the prefix value refers.

Claim 26, upon which claims 35 and 42-51 depend, is directed to an apparatus that includes a transmitter configured to forward a prefix value to a node in a packet switched environment to create a security association with the node based on the prefix value. The prefix value may refer to a portion of a first internet protocol address, where the security association is valid for a plurality of different internet protocol addresses. Additionally, each of the plurality of internet protocol addresses comprises the portion of the first internet protocol address to which the prefix value refers.

Application No.: 10/615,419

Claim 29 is directed to an apparatus that includes forwarding means for forwarding a prefix value to a node in a packet switched environment to create a security association with the node based on the prefix value. The prefix value refers to a portion of a first internet protocol address, where the security association is valid for a plurality of different internet protocol addresses. Additionally, each of the plurality of internet protocol addresses comprises the portion of the first internet protocol address to which the prefix value refers.

Claim 31, upon which claims 37 and 52-57 depend, is directed to an apparatus that includes a receiver configured to receive a prefix value from a node in a packet switched environment. The prefix value may refer to a portion of a first internet protocol address. The apparatus also comprises a creation unit configured to create a security association between the node and the apparatus based on the prefix value, where the security association is valid for a plurality of different internet protocol addresses. Each of the plurality of internet protocol addresses comprises the portion of the first internet protocol address to which the prefix value refers.

Claim 32 is directed to an apparatus that includes receiving means for receiving a prefix value from a node in a packet switched environment. The prefix value may refer to a portion of a first internet protocol address. The apparatus also includes a creation means for creating a security association between the node and the apparatus based on the prefix value, where the security association is valid for a plurality of different internet protocol addresses. Additionally, each of the plurality of internet protocol addresses

Application No.: 10/615,419

comprises the portion of the first internet protocol address to which the prefix value refers.

Claim 38, upon which claim 39 depends, is directed to a method that includes receiving a prefix value from a node in a packet switched environment. The prefix value may refer to a portion of a first internet protocol address. The method also includes creating a security association with the node based on the prefix value, where the security association is valid for a plurality of different internet protocol addresses, and each of the plurality of internet protocol addresses comprises the portion of the first internet protocol address to which the prefix value refers.

Claim 40 is directed to a computer program embodied on a computer-readable medium, the computer program configured to control a processor to perform operations. The operations comprise receiving a prefix value from a node in a packet switched environment. The prefix value may refer to a portion of a first internet protocol address. The operations also comprise creating a security association with the node based on the prefix value, where the security association is valid for a plurality of different internet protocol addresses, and each of the plurality of internet protocol addresses comprising the portion of the first internet protocol address to which the prefix value refers.

Claim 41 is directed to a computer program embodied on a computer-readable medium, the computer program configured to control a processor to perform operations. The operations comprise forwarding a prefix value to a node in a packet switched environment to create a security association with the node based on the prefix value. The

Application No.: 10/615,419

prefix value may refer to a portion of a first internet protocol address, where the security association is valid for a plurality of different internet protocol addresses, and each of the plurality of internet protocol addresses comprising the portion of the first internet protocol address to which the prefix value refers.

Each of claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 recites limitations that are not disclosed or suggested by Pirttimaa.

Pirttimaa discloses a method and network element for providing secure access to a packet data network. In Pirttimaa, a first source information is derived from a message received from a terminal device. The first source information is compared with a second source information derived from a packet data unit used for conveying the message, or derived from a security association set up between the terminal device and the data network. A protection processing for protecting the packet data network from a fraudulent user attack is then initiated based on the comparing result.

However, Pirttimaa fails to disclose or suggest all the limitations of any of the pending claims. For example, Pirttimaa fails to disclose or suggest "forwarding a prefix value to a node in a packet switched environment to create a security association...based on the prefix value, said prefix value referring to a portion of a first internet protocol address, wherein the security association is valid for a plurality of different internet protocol addresses, each...comprising said portion of the first internet protocol address to which the prefix value refers," as recited in claim 1, and as similarly recited in claims 26, 29, and 41, though each claim has its own scope. Similarly, Pirttimaa fails to disclose or

suggest "receiving a prefix value...referring to a portion of a first internet protocol address; and creating a security association...based on the prefix value; wherein the security association is valid for a plurality of different internet protocol addresses, each...comprising said portion of the first internet protocol address to which the prefix value refers," as recited in claim 38, and as similarly recited in claims 31-32 and 40, though each claim has its own scope. Instead, Pirttimaa discloses providing secure access, where a first source information, derived from a message received from a terminal device, is compared with a second source information, derived from a packet data unit used for conveying the message or a security association set up between the terminal device and the data network.

The Office Action has taken the position that these features are disclosed in paragraphs [0039]-[0042] of Pirttimaa. However, a review of these portions of Pirttimaa demonstrates that Pirttimaa fails to disclose or suggest the limitations recited above. For example, paragraph [0039] discloses:

> FIG. 2 shows a message signaling and processing diagram indicating the protection mechanism according to the preferred embodiments. Initially, a setup procedure for setting up a security association (SA) between the P-CSCF 30 and the UE1 40 is performed as specified in the 3GPP specification TS 33.203. The SA setup procedure is necessary in order to decide what security services are applied and when the security services start. For protecting IMS signaling between the UE1 40 and the P-CSCF 30, it is necessary to agree on shared keys provided by an IMS Authentication and Key Agreement (AKA) function, on certain protection methods (e.g. an integrity protection method) and a set of parameters specific to a protection method, e.g. the cryptographic algorithm to be used. The parameters negotiated are typically part of the SA to be used for a protection method. In particular, the UE1 40 and the P-CSCF 30 agree on an integrity key to be used for integrity protection. The mechanism is based on the IMS AKA. Then, the UE1 40 and the P-CSCF 30 both verify that received data or messages originate from a node which has the agreed integrity key. The identity used for authenticating a subscriber is the IMPI.

In light of the above, paragraph [0039] of Pirttimaa discloses that a security association is initially setup "to decide what security services are applied" and to "agree on shared keys provided by an IMS Authentication and Key Agreement (AKA) function." However, paragraph [0039] does not disclose a "prefix value," "forwarding a prefix value...to create a security association," or a "prefix value referring to a portion of a first internet protocol address," as recited in claim 1. Similarly, paragraph [0039]of Pirttimaa fails to disclose that the "security association is valid for a plurality of different internet protocol addresses, each...comprising said portion of the first protocol address to which the prefix value refers," as is also recited in claim 1. Instead, paragraph [0039] discloses that a security association is initially set up to decide security services and keys.

In paragraph [0040], Pirttimaa discloses that while only one security association is active between the user and the P-CSCF, the security association can be updated when a new successful IMPU authentication re-registration has occurred.

> [0040] Only one SA is active between the UE1 40 and the P-CSCF 30. This single SA is updated when a new successful authenticated re-registration has occurred. Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered, the UE1 40 sends a SIP REGISTER message towards the SIP registrar server, i.e. the S-CSCF 10, which will perform the authentication of the user. The P-CSCF 30 forwards the SIP REGISTER message towards the S-CSCF 10 and adds a Via header with its address included. Upon receiving the SIP REGISTER message the S-CSCF 10 needs one authentication vector (AV). Based on the parameters given in the AV, the S-CSCF 10 authenticates the user and registers the corresponding IMPU. Implicitly registered IMPUs can be delivered by the HSS 20 to the S-CSCF 10.

As such, paragraph [0040] discusses updating a security association may be updated when an IMPU for an IP multimedia protocol is re-registered. However,

- 18 -   Application No.: 10/615,419

paragraph [0040] does not disclose or suggest a "prefix value," "said prefix value referring to a portion of a first internet protocol address," or "forwarding a prefix value...to create a security association based on the prefix value," as recited in claim 1. Similarly, paragraph [0040] of Pirttimaa fails to disclose that the "security association is valid for a plurality of different internet protocol addresses, each...comprising said portion of the first internet protocol address to which the prefix value refers." Indeed, paragraph [0040] has nothing to do with a relationship between a "prefix value," a "security association," and a "plurality of different protocol addresses," let alone the relationship described by the limitations of claim 1. Instead, paragraph [0040] merely discloses that a security association can be updated when an IMPU is re-registered.

In paragraph [0042], Pirttimaa discloses an address comparison that occurs when a P-CSCF receives an INVITE message from a user.

> [0042] When a SIP request message, e.g. an INVITE message is send from the UE1 40 to the P-CSCF 30 (step 1), the P-CSCF 30 performs an address comparison (step 2) in which an IP address or at least a part (e.g. a unique prefix) of the IP address, which is derived from a received IP datagram conveying the SIP message (if IPSec is used) or derived from a database (if SIPSec is used), is compared to an IP address indicated in a header, e.g. contact header or any other header portion, of the SIP message. As an example, the contact header of the SIP message is used to indicate the point of presence for the subscriber, i.e. the IP address of the UE1 40. This is the temporary point of contact for the subscriber which is being registered. Subsequent requests destined for the subscriber will be send to this address. Thus, this information is stored in the P-CSCF 30 and the S-CSCF 10.

As such, paragraph [0042] discloses that an address comparison occurs when the P-CSCF receives an INVITE message from a user. The comparison is between an IP address in the INVITE message and an IP address that is either in the datagram conveying the INVITE message or stored in a database. Either way, not only does

Application No.: 10/615,419

paragraph [0042] fail to disclose the "forwarding," the "prefix value," and the "security association" discussed above, but paragraph [0042] is irrelevant to claim 1 because the processes discussed in paragraph [0042] all occur after a security association is negotiated (see paragraph [0041]). By contrast, embodiments of the claimed invention are directed to the security association creation process. Accordingly, contrary to position taken by the examiner, paragraphs [0039]-[0040] and [0042] of Pirttimaa fail to disclose or suggest all the limitations of claims 1, 26, 29, 31-32, 38, and 40-41.

As such, it is clear that Pirttimaa fails to disclose or suggest "forwarding a prefix value to a node in a packet switched environment to create a security association...based on the prefix value, said prefix value referring to a portion of a first internet protocol address, wherein the security association is valid for a plurality of different internet protocol addresses, each...comprising said portion of the first internet protocol address to which the prefix value refers," as recited in claim 1, and as similarly recited in claims 26, 29, and 41. Indeed, the claimed relationship between the "prefix value," the "security association," and the plurality of internet protocol addresses" is simply not disclosed by Pirttimaa. For example, Pirttimaa simply does not disclose that a prefix value referring to a portion of a first internet protocol address may be forwarded to a node to create a security association that is valid for a plurality of internet protocol addresses that each include the portion of the first internet protocol address that refers to the prefix value, which is of no surprise as Pirttimaa is not concerned with such features.

In light of the above, Applicants respectfully assert that Pirttimaa fails to disclose or suggest all the limitations of claims 1, 26, 29, 31-32, 38, and 40-41. Similarly, Applicants respectfully assert that Pirttimaa fails to disclose or suggest all the limitations of claims 2-3, 5-8, 12, 28, 33, 35, 37, 39, and 42-57. Consequently, claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 are not anticipated by Pirttimaa under 35 U.S.C. § 102(e). Therefore, Applicants respectfully request that the rejection of claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 be withdrawn.

Further, it should be noted that the Office Action is deficient because it fails to clearly set forth the status of claim 3. 37 C.F.R. § 1.104(b) mandates that an Office Action must be complete as to all matters. MPEP § 707.07(f) further states that "[i]n order to provide a complete application file history and to enhance the clarity of the prosecution history record, an examiner *must* provide clear explanations of all actions taken by the examiner during prosecution of an application" (emphasis added). MPEP 707.07(d) indicates that, "Where a claim is refused for any reason relating to the merits thereof it should be 'rejected' and the ground of rejection fully and clearly stated, and the word 'reject' must be used. The examiner should designate the *statutory basis* for any ground of rejection by express reference to a section of 35 U.S.C. in the opening sentence of each ground of rejection."

In the instant case, while page 4 of the Office Action seems to compare Pirttimaa to claim 3, the Office Action fails to clearly indicate the status of claims 3. For example, in the Office Action Summary, the status of claim 3 is not presented. Additionally, on

Application No.: 10/615,419

page 4, the Office Action states that "Claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Prittimaa (US PGP No. 20030154400)," which does not include claim 3. Accordingly, it is unclear whether the Office Action intended to reject claim 3 under 35 U.S.C. § 102(3) as being anticipated by Pirttimaa, or if, during the preparation of the Office Action, the rejection of claim 3 was considered, but ultimately decided against. At any rate, the Office Action fails to be "complete as to all matters" and to "enhance the clarity of the prosecution history record" for failing to "provide clear explanations of all actions taken by the examiner," as required by the MPEP. Moreover, even if claim 3 were rejected under 35 U.S.C. 102(b) as being anticipated by Pirttimaa, Applicant traverses such a rejection on the grounds that Pirttimaa, as discussed above, fails to disclose or suggest all the limitations of claim 3, for its dependency from claim 1, and for the limitations recited therein. Therefore, Applicant respectfully requests that the pending claims be allowed, or, in the alternative, that a new Office Action be provided that clearly sets forth the status of claim 3.
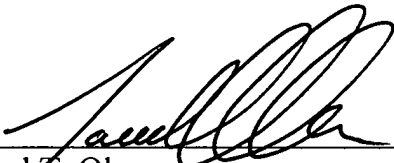
In light of the above, it is clear that the specification provides ample support for a "computer-readable medium," as recited in claims 40-41. Additionally, it is clear that Pirttimaa fails to anticipate any of claims 1-2, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57. Therefore, Applicants respectfully request that the pending objections and rejections be withdrawn, and that claims 1-3, 5-8, 12, 26, 28-29, 31-33, 35, and 37-57 be allowed.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Jared T. Olson
Registration No. 61,058

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

JTO:skl:dlh:kh

Enclosures: Petition for Extension of Time
            Check No. 20654